17. The Quadratic Sieve and Elliptic Curves

17.a The Quadratic Sieve

Sieve methods for finding primes or for finding factors of numbers are methods by which you take a set P of prime numbers one by one, and observe which of a large set, S, of numbers are divisible by each one of them.

For finding primes by the linear sieving method you seek numbers that are not divisible by any of the prime numbers in P (which you usually take to be the first k primes.)

For factoring, instead we want numbers **whose squares mod N are completely factorable by primes in P.** (This means that all the prime factors of N are in our set P)

Why? because
if we can find enough of these we can find a combination of them, call it q, whose square is a perfect square mod N.

If we do this, at least half the time q will be different from the square root of its square we can determine. We may then find two numbers x and y that both have the same square but are neither identical nor negative of one another (when N is neither a prime nor a prime power) and from these we can factor.

How?

If N=p*q, and x and y are given mod p and mod q as (a,b) and (a,-b), then x+y and x-y will be congruent to 0 mod p or mod q and Euclid's algorithm applied to either one will produce p or q as its greatest common factor with N. And if x and y have the same square mod N and are not the same or minus one another, they will have this form.

Before attempting to go about seeking such numbers, let us ask: how many numbers have the property of being factorable into small prime factors? or into prime factors all of which are at most among the first k primes? or into primes less than Q?

The number z will be factorable by the first k primes if it has no prime factor larger than the largest of these which we will call Q, but z is not itself a prime.

We can estimate how common such numbers are by noting that the probability of a number being divisible by a prime p is (1-1/p) and the density of primes among numbers of size

roughly t is on the order of 1/lnt.

The probability that a given number z has no prime factors above Q is then the product over all primes p between Q and z/2 of (1-1/p). If we take the log of this product approximate each term in it by -1/p, and sum them we will find that the natural logarithm of this probability is on the order of the integral from Q to z/2 of the density of primes p of size x times -1/x, which is on the order of -òdx/(xln(x)) or -ln(ln(z/2)+ln(ln(Q)) or ln(lnQ/ln(z/2)). This tells us that the probability of not being so divisible is the exponent of this or log Q/log (z/2) (the base of the logarithm is irrelevant). Thus, if we use primes up to a million and z has 100 decimal digits we expect this probability to be of the order of 6/100 or 1 out of 20 or so. some of these will be primes, but by the same argument we can estimate the number of these by replacing z/2 by the square root of z and replacing Q by a small number like 1.

The upshot of all this is that there are quite a few numbers that will be factorable into small prime factors even if they are quite large.

So how do we use sieving to find such numbers?

We will test whether one particular number, y, has a square that is divisible by each of the first k primes. We make this square as small as we can by choosing y to be near the square root of aN, for a small integer a, in fact usually for a=1. If so, y's square will be not far from a^2N and the square can be represented as either plus or minus a number, call it t. since we can choose y to be within a half of the square root of N we can make the order of magnitude of t something like $N^{1/2}$ or less, (because $(N^{1/2}+w)^2 \bmod N = w^2+2wN^{1/2}$ which for w less than 1/2 is at most $N^{1/2}+1/4 \bmod N$.) Thus we have $y^2 \circ t \bmod N$ and both y and t are on the order of $N^{1/2}$.

To get this far, we have to divide a number that is on the order of $N^{1/2}$ by all of the primes in P. This is requires lots of work if we make P big and N is very big. But we get y and t mod every prime in P as defined above and they are both on the order of $N^{1/2}$.

We next examine the numbers y+j and their squares mod N

We find that $(y+j)^2 = y^2 + 2*j*y + j^2 \circ t + 2*j*y + j^2 \bmod N$.

We can therefore generate these numbers mod any of our primes from t and y mod that prime. Each time we increase j by 1(from j to j+1) e need add 2*y+2*j+1 to the previous number mod that prime.It is not so much work to increase j.

We are now looking to find that $((y+j)^2 \bmod N$ is a product of powers of the primes in P.

We are interested in the question: is $(y+j)^2$ divisible by p, and we want to know this

for each of our primes p. This is equivalent to the statement that $(t+2jy+j^2)$ mod N) is congruent to 0 mod p. This is a quadratic equation in j mod p, which we know will have solutions in either 0 or two congruence classes mod p.

And we can find which congruence classes mod p obey it by writing it out mod p (which involves finding t and y
mod p) and checking each congruence class. Roughly half the time it will have no solutions and we can forget about the prime (unless we start again with a different value of y). Otherwise we will find two (or perhaps 1) good congruence classes for each prime. A good congruence class for j for a particular prime will be one for which this equation holds.

By checking these things, we can find the "good congruence classes" (those that such that the prime divides $(y+j)^2$ mod N without remainder for all our primes.

Now we go through our j values and divide $(y+j)^2$mod N by each prime p that divides it until the quotient is relatively prime to p; continue this for all the good congruence classes to which it belongs. In this way we can factor it as much as it can be factored by our primes.

If $(y+j)^2$ mod N is completely factored by our primes, we have won a battle, and add y+j to our list of “numbers with squares mod N completely factorable by primes in P.

In this way we try to construct a large number of numbers that have factorable squares mod N, that is have squares all of whose prime factors are among our k primes.

We now turn to the question: what can we do with these numbers?

For each number z on our list we construct a binary vector v(z) whose jth component is 1 if z^2mod N is divisible by p_j^{aj} where aj is an odd integer, and is not divisible by p_j^{aj+1}.

Our next goal is to find a linear dependence among these vectors mod 2. Suppose we find one. Suppose for example we have

$$v(z1)+v(z2)+\ldots + v(zs) \circ 0 \text{ mod } 2.$$

This implies that the product $(z1*z2*\ldots*zk)^2$ can be written as a perfect square mod N, which square is obtained by a method which does not know about how we got it. Thus, while half the time the square root of that perfect square may be plus or minus (z1*z2*…*zk), half the time it will not be, and we will be able to factor N.

Consider the following example:

Suppose we seek to factor 2047. We find that $(2047)^{1/2}$ is between 45 and 46. We then choose y=45 and find $n-y^2$ =2047-2025=22.

We define y mod p to be y(p) and t mod (p) to be t(p).

We notice then that y(2)=1; t(2)=0; let q(j) = t + 2*j*y + j^2mod N
This implies q(j) º j^2 mod 2, so that q(j) is divisible by 2 for all even j.
Similarly we get y(3)=y(5)=0; t(3)=1, t(5)=2, and we get
q(j) º j^2 –1 mod 3, which vanishes for j=1 or 2 mod 3
q(j) º j^2 –2 mod 5, which never vanishes.
Similar analysis can be applied for each prime. We list the first few results

P	y(p)	t(p)	equation	congruence classes solving it
7	3	1	j^2-j-1=0	none
11	1	0	j^2+2j=0	0, 9
13	6	9	j^2-j +4 =0	none

The following table from gives the values of q(p) for j=1 to 11
The first column gives the value of j the second give q(j) and the rest give q(j) mod 2,3,5,7,11,13, and 17.

0	22	0	1	2	1	0	9	5
1	**69**	1	0	4	6	3	4	1
2	**162**	0	0	2	1	8	6	9
3	257	1	2	2	5	4	10	2
4	354	0	0	4	4	2	3	14
5	453	1	0	3	5	2	11	11
6	554	0	2	4	1	4	8	10
7	657	1	0	2	6	8	7	11
8	762	0	0	2	6	3	8	14
9	869	1	2	4	1	0	11	2
10	978	0	0	3	5	10	3	9
11	**1089**	1	0	4	4	0	10	1

The only primes that interest us here are 2 3 and 11 since the others never are 0.

The only numbers that are completely factorable here are 162 and 1089 corresponding to j=2 and 11 and y+j
= 47 and 56 respectively. The binary vectors we get for these three primes (mod 2) are respectively
(1,0,0) and (0.0,0). The number 1089 corresponds to j=11 in this table and to the vector (0,0,0), which is linearly dependent in itself!. This means that 1089 is a square in itself: it completely factors into 3*3*11*11. Thus we can claim that y+11 or 56 has the same square as 33 mod 2047. We then find that 89 and 23 are factors of 2047, by using Euclid's Algorithm

starting from N, which is here 2047 and 56-33, or 23, (or 56+33 which is 89).

Normally when N is very large, in this procedure you will not reach a j value that causes q(j) to go above N.
If you do, as you might here, you must choose a new y (one near the square root of 2N say) and compute the new t and repeat the process Notice that for j=2 162 factors into 2*(3^4)
.

In general, when there are more vectors than components (here primes) there must be a linear dependence and an opportunity for factoring.

This method is as good as any known, I think, for factoring. But there are other ways. The questions as to how long this algorithm takes to work are: given N, how many primes should you put in P? Given that number, how far do you have to go to reach enough numbers completely factorable by these primes, to get enough to find a linear dependence among the corresponding vectors?

We will not pursue these questions here.

22b. The Elliptic Curve Method for Factoring

Elliptic curves can be used for factoring, and they can also be used for encoding. So what is an elliptic curve?

If is the locus of solutions of a polynomial equation in two variables, say x and y, that is quadratic in y and cubic in x. We will consider such solutions mod N, where N is a the product of two prime numbers, say p and q. As usual, by the Chinese Remainder Theorem, we can understand what is going on separately mod p and mod q.

Here is an example of such an equation

$$y^2 = x^3 + a\,x^2 + bx + c.$$

Notice that here if we fix x, then solutions, if they exist, are plus and minus the square root of what ever the right hand side comes out to be.

So one question is, what numbers mod p are squares?. It turns out, that of the non-zero remainders on dividing by a prime other than 2, half are squares and half are not.

(Think of it this way: every remainder has a square so there are p-1 squares all together,

and +a and –a have the same square, so there can be at most (p-1)/2 distinct non-zero squares. And we know that the quadratic equation $x^2 = a^2$ can have at most two solutions in a field, by the fundamental theorem of algebra which means there must be at least (p-1)/2 distinct non-zero squares mod p.)

The squares are called "quadratic residues" mod p. This means for us, that roughly half the possible x values will product a right hand side here that is a quadratic residue, and otherwise it wont. This means that the number of solutions to our equation will be roughly p (two for each of roughly half the possible x values for which we get a quadratic residue on the right.)

.
As a matter of fact, the number of solutions typically behaves somewhat randomly and so typically differs from p by something of the order of $p^{1/2}$.

And why do we care?

\

The wonderful thing is the solutions here, with the addition of an artificial identity element, define a group, so that each equation of this form defines a group mod p whose size is somewhat randomly chosen roughly between $p-2p^{1/2}$ and $p+2p^{1/2}$

And that raises four questions:

1. What is this group?

2. What good does it do us?

3. Can we actually do what is required to exploit this goodness?

4. How long might this take?

The first question is really: what is the multiplication table for this group? We can answer that by giving a rule for finding the product of two distinct roots $A= (x_a, y_a)$ and $B=(x_b, y_b)$ of the equation, and also for finding the square of a root.

There is a neat geometric answer to these questions, which is easily translated to algebra.

The answer to the first is this. Suppose we draw a line connecting the point A and B in the plane. This line will always intersect the elliptic curve at some other point, call it C' (or $x_{c'}, y_{c'}$). Then the product of A and B is gotten by reversing the sign of y_c in C'. If we call the product C we have $C=(x_{c'}, - y_{c'})$. To repeat, the product of A and B is the reflection about the

x axis of the third solution of our equation on the line containing A and B.

And what is the product of A with itself? We find the second point on the line through A tangent to our elliptic curve, and reverse that about the x axis.

The identity is an imaginary point taken to be on any line perpendicular to the x axis.

What is the inverse of A? it is the solution that is its reflection. Their product is the reflection of the identity (still the identity)

Notice by the way, when you take the "product" in this group and get the identity, the factors must lie on the same vertical line, and hence have the same x value. This will be interesting to us later.

So we have a group, of some unknown size, and you can start with any particular pair x and y and a given a and b in the equation and adjust c to make the pair (x,y) into a solution, which we call A.

What can we do with this? Well we hope that the size, call it S, of our group has only prime factors under M (say a million,) and even more, that the size of the group is a divisor of M!. This will usually be true if all the factors of S are less than M.

Then the order of the subgroup of S generated by the element A (all computations considered modp) (remember that this subgroup consists of all of the powers of A) must be a divisor of the order of S, and hence a divisor of M!. This means that if we raise A to the M! power, we get the identity element of the group, which is the artificial point on every vertical line. To do this, we multiplied some solution B by its reflection in y.

We will see that when we do this mod N, we will trying to divide by 0 mod p. Now we divide by using Euclid's algorithm to find the inverse of our divisor, and then multiply by it. When we try to divide by 0 mod p, Euclid's algoritm will spit out the value of p as a gcd as it fails to find the inverse of the 0 denominator mod p.

The upshot of all this is that if we raise A successively to the powers j! in our group, (in which all calculations are mod N) for j = 1 up to M, at some point the factor p of M will pop out as a gcd in an application of Euclid's algorithm

(we of course assume that this does not happen simultaneously in q as well, but that is a very rare thing to happen.).

And what happens if neither the size of the group mod p nor mod q is a product of "small primes"? Then we will have to start again with another equation. Of course that can be done in parallel on a different machine.

We now ask, how hard it is to do all this? Namely to raise A to a factorial power in the group of solutions of our equation, or rather to do so mod N.

The first question is how hard is it to multiply two distinct group elements, say A and B, where multiply means apply the operation of the group (which is finding the third solution point on the line containing A and B and changing the sign of the y component.)

A and B and C' must not only obey our equation, $y^2 = x^3 + ax^2 + bx + c$, but also obey

$$y - y_a = ((y_b - y_a)/(x_b - x_a))^* (x - x_a).$$

because this equation defines the line containing A and B. We can substitute this linear formula for y into our original equation, and get a cubic equation for x with no y in it.

The coefficient of x^2
will be minus the sum of the roots of this equation, and since we know two of them, we can read off what the third one is; it turns out to be

$$x_c = m^2 - a - x_a - x_b,$$

where m is the slope of the linear equation, which is $((y_b - y_a)/(x_b - x_a))$.

And the y component of C can be read off once we know x_c. So our only problem is computing m, which involves dividing by $(x_b - x_a)$ This we accomplish by finding the inverse of $(x_b - x_a)$ mod N by use of Euclid's algorithm using this number and N. (notice what happens if this difference is 0 mod p)

To square A we have to compute the slope m differently, and everything else is the same. The straight line is chosen to have the same slope as our curve which is dy/dx which we can easily see is $(3x_a^2 + 2ax_a + b)/2y_a$.

Thus every multiplication requires one division and hence one use of Euclid's algorithm with N.

Strangely enough the rough estimate of how much effort is required to apply this method is similar to the previous one.

Euclid's algorithm does take lots of effort, and it must be performed lots of times one after another, so it is harder to do lots of things in parallel with this method than with the quadratic sieve.

To me it is wonderful that there is a group like the one associated with an equation here, and that it is possible to exploit the apparent somewhat randomness of its size to actually factor numbers.